

(19) World Intellectual Property Organization
International Bureau



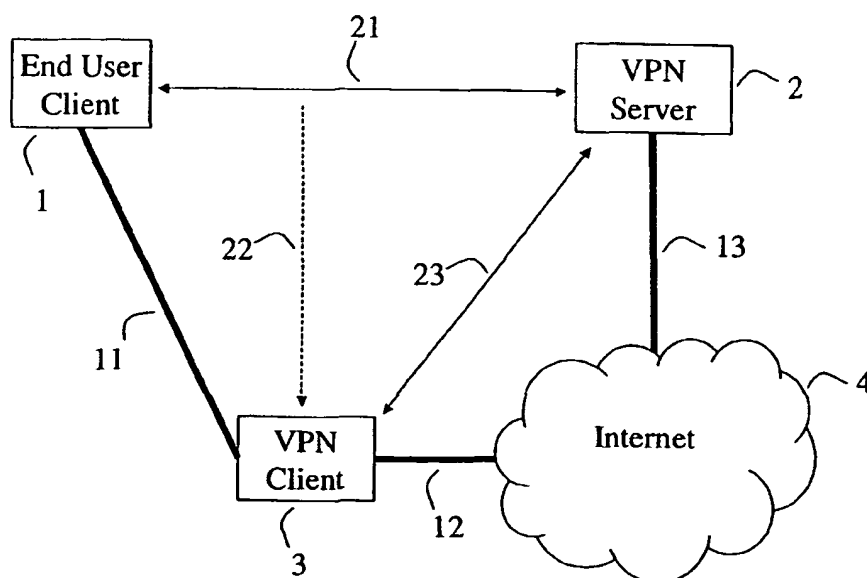
(43) International Publication Date
9 January 2003 (09.01.2003)

PCT

(10) International Publication Number
WO 03/003660 A1

- (51) International Patent Classification⁷: **H04L 12/28**, 12/56, 12/46 (74) Agents: **SOHLMAN, Leif** et al.; Telia Reseach AB, Koncernpatent, S-123 86 Farsta (SE).
- (21) International Application Number: **PCT/SE01/01472** (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (22) International Filing Date: 27 June 2001 (27.06.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (71) Applicant (*for all designated States except US*): **HYGLO AB** [SE/SE]; Västberga Alle' 60, S-126 75 Hägersten (SE). (84) Designated States (*regional*): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- (72) Inventors; and
- (75) Inventors/Applicants (*for US only*): **BYSTRÖM, Leif** [SE/SE]; Tegelbruksvägen 37, S-126 34 Hägersten (SE). **AHLARD, David** [SE/SE]; Sandfjärdsgatan 105, S-120 56 Årsta (SE). **BERGKVIST, Joakim** [SE/SE]; Barks väg 12, S-170 73 Solna (SE). **HANSSON, Urban** [SE/SE]; Porlabacken 27, S-124 70 Bandhagen (SE).
- Published:
— with international search report
- For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

(54) Title: SYSTEM AND METHOD FOR ESTABLISHMENT OF VIRTUAL PRIVATE NETWORKS USING TRANSPARENT EMULATION CLIENTS



(57) Abstract: System for establishment of a virtual private network connection, comprising an end user client device (1) and a VPN access server (2) communicatively connected to the end user client via the Internet (4). The system is characterised in that it includes a standalone VPN client (3) device physically interconnecting (11, 12, 13) the end user client with the Internet, said VPN client comprising monitoring means for monitoring all traffic between the end user client and the VPN server. Preferably said monitoring means are devised to detect when a handshake agreement is established between the end user client and the VPN server, and to overtake a VPN setup session for said end user client upon detection of said handshake agreement.

WO 03/003660 A1

SYSTEM AND METHOD FOR ESTABLISHMENT OF VIRTUAL PRIVATE NETWORKS USING TRANSPARENT EMULATION CLIENTS

5 Field of the invention

The invention relates in general to computer networks, and in particular to systems and methods for in customer premises equipment based network access servers for secure, dynamic, and fault tolerant establishment of server controlled Internet Protocol virtual private networks.

10

Background

Most enterprises are located at multiple sites where each site has its own local area network (LAN). A site is defined as anything from a head-quarter, or an affiliation company site, to a single employee's remote office site. Some kind of communication infrastructure is then used to interconnect the different sites. The Internet evolution can roughly be categorised into two main areas:

- 15 a) Internet as the global communication infrastructure. Traditionally, companies used so called leased lines, provided by telephone companies to interconnect their sites. Separated firewall solutions were used for accessing the Internet. During the last years, companies are no longer using Internet only for external communication, more and more companies are trying out new network solutions that enables them to also use Internet for company-internal communication. Internet has become their site-to-site interconnecting medium.
- 20 b) Broadband Internet access. In parallel with the above, more and more broadband access solutions are rolled out by different network access providers. This enables anyone to upgrade their access to Internet from a traditional dial-up PSTN/ISDN (Public Switched Telephone Network/Integrated Services Digital Network) access solution to a broadband solution, e.g. ADSL (Asymmetric Digital Subscriber Line), Cable or Ethernet, with direct access to Internet. Apart from the obvious broadband benefits, the network access user is also able to always be connected to the Internet.

The common name for most of the network solutions that interconnects multiple sites over Internet is "virtual private networks" (VPN). VPNs can be implemented in numerous ways, this is well explained in e.g. the IETF by B. Gleeson et. al, "A Framework for IP Based Virtual private Networks", RFC 2764, February 2000, where IP stands for Internet Protocol. A VPN is a private network that is configured within a public network. For years, common carriers have built VPNs that appear as private national or international networks to the customer, but physically share backbone trunks with other customers. VPNs enjoy the security of a

private network via access control and encryption, while taking advantage of the economies of scale and built-in management facilities of large public networks. Today, there is tremendous interest in VPNs over the Internet, especially due to the constant threat of hacker attacks. The VPN adds that extra layer of security, and a huge growth in VPN use is expected. In general, the different VPN solutions can be categorized into two main groups; customer premises equipment (CPE) based solutions or network based solutions.

The Internet is a public data network based on network paradigms such as equal and best effort traffic treatment. All traffic crossing the Internet is public and insecure resulting in a number of problems that need to be solved, e.g. end-to-end security communication between enterprise sites. Some problems have solutions supported by several VPN system vendors, such as encrypted IP tunnelling between end-users using the IPSec architecture described by S. Kent and R. Atkinson in "Security Architecture for the Internet Protocol", RFC 2401, November 1998, or stand-alone firewall solutions, desktop software VPN clients. e.g. Microsoft® VPN, etc. A PC that is connected to the Internet can, not easily but it is possible, be used as a transit node by a hacker, e.g. the hacker could use a Trojan horse program to get inside the PC. Well inside, the Trojan horse program may be adapted to release application software that will act as some authenticated software installed by the owner of the PC. It is very difficult for layer- 2 and 3 firmware/software to detect this kind of malicious applications. Therefore, it is recommendable to have VPN control and management software and firmware functions and end-user applications, such as service login software, "authenticated" software applications that in some way uses the network infrastructure provided by the VPN service, separated on different hardware platforms. What generally should be avoided, is having PC clients that are responsible for configuring the actual VPN setup, i.e. having access to the lookup-table for other VPN members public IP addresses, having access to information on how to authenticate, perform integrity check and encrypt traffic aimed for the VPN etc.

Summary of the invention

According to a first aspect of the invention, a system is provided for establishment of a virtual private network connection, comprising an end user client device and a VPN access server communicatively connected to the end user client via the Internet. The system is characterised in that it includes a standalone VPN client device physically interconnecting the end user client with the Internet, said VPN client comprising monitoring means for monitoring all traffic between the end user client and the VPN server. Preferably said monitoring means are devised to detect when a handshake agreement is established between the end user client and

the VPN server.

Said VPN client comprises, in one embodiment, session overtaking means, devised to overtake a VPN setup session for said end user client upon detection of said handshake agreement. Preferably the end unit client side of the VPN client is defined as a secure domain, and the Internet and server side of the VPN client is defined as an insecure domain, said VPN client being devised only to accept a request for a VPN session setup when initialised from said secure domain.

In one embodiment said monitoring means are devised to determine said handshake agreement for the VPN setup session as completed upon detecting that said server acknowledges a VPN setup request that has been initialised by said end user client. Said VPN client may be devised to request, upon detection of a completed handshake, said server to distribute VPN configuring data relevant for the inclusion of said end user client into said virtual private network.

In one embodiment said VPN client is devised to undertake a proxy roll, comprising means for acting as a VPN server proxy towards the end user client, and means for acting as an end user client proxy towards the VPN server.

According to a second aspect, the present invention provides a method for establishing a connection for comprising an end user client device to a virtual private network controlled by a VPN access server communicatively connected to the end user client via the Internet, comprising the steps of providing a standalone VPN client device physically interconnecting the end user client with the Internet, and monitoring all traffic between the end user client and the VPN server by means of monitoring means in said VPN client. Preferably said monitoring means detects when a handshake agreement is established between the end user client and the VPN server, wherein said VPN client overtakes a VPN setup session for said end user client upon detection of said handshake agreement.

In one embodiment the end unit client side of the VPN client is defined as a secure domain, and the Internet and server side of the VPN client is defined as an insecure domain, said VPN client only accepting a request for a VPN session setup when initialised from said secure domain.

Preferably said monitoring means determine said handshake agreement for the VPN setup session as completed upon detecting that said server acknowledges a VPN setup request that has been initialised by said end user client. In one embodiment said VPN client requests, upon detection of a completed handshake, said server to distribute VPN configuring data relevant for the inclusion of said end user client into said virtual private network. In one embodiment said VPN client undertakes a proxy roll, acting as a VPN server proxy towards the end user client, and acting as an end user client proxy towards the VPN server.

Brief description of the drawings

Preferred embodiments of the invention are described below with references being made to the drawings, on which

5 Fig. 1 illustrates the system overview according to an embodiment of the present invention;

Fig. 2 illustrates traffic monitoring and session overtaking according to an embodiment of the present invention; and

10 Fig. 3 illustrates an emulated LAN on top of a global IP network, according to an embodiment of the invention.

Detailed description of preferred embodiments

According to one aspect, the system according to the present invention is based on a standard IP network like the public Internet. The system comprises multiple
15 VPN clients and at least one server. One server can be a distributed cluster of physical boxes. The VPN clients could be implemented as drivers on the client computer but are for security reasons preferably implemented in a stand alone hardware box. A purpose of this mechanism is to establish dynamic and secure Virtual Local area Networks between some or all of the clients. A virtual network is
20 created by establishing connection groups in a VPN server. The server has a service device for keeping track of connected machines and mapping them to IP addresses. In one embodiment this is obtained using ARP (Address Resolution Protocol), an IP protocol used to obtain a node's physical address. A client station sends an ARP request to the VPN server with the VPN internal IP address of the target node it
25 wishes to communicate with, and the VPN server responds by sending back the external IP address so that packets can be transmitted. ARP returns the layer-2 address for a layer-3 address. This mechanism also handles distribution of public keys to form complete security associations. For handling broadcasts an emulated broadcast service is implemented in the server, preferably using an IP multicast
30 group or as a separate broadcast service. Data sent directly from one machine in the virtual network to another is tunnelled over IP directly to the IP address of the receiving client. The mechanism includes both the case where data packets are tunnelled directly over IP and when an layer-2 media such as Ethernet is bridged onto the IP network.

35 Fig. 3 illustrates an embodiment of the system according to the present mechanism, wherein a network 4 comprises five nodes; four VPN clients 31 - 34 with global addresses C1 - C4, and a server S. All of these are connected to and have a valid address in the physical network 4. These nodes are interconnected using standard Internet routing procedures, but the clients 31 - 34 are not on the

same LAN. On top of this network infrastructure, clients 31, 32 and 33 form a virtual network 30 with local addresses D1, D2 and D3. In the illustrated case the clients in this VPN appear to be on the same local area network. The reason for this is the broadcast service, i.e. the service device, which delivers all packets for the local broadcast domain to all machines on the VPN 30. Thus service discovery mechanisms or layer-2 ARP operate transparently on top of the virtual network. When client 31 on the VPN wants to transmit a packet directly to client 32 the client-software requests the physical address C2 from server S, based upon the local address D2, and possible security keys required for talking to D2 from S. D1 is then able to transmit the packet in a secure tunnel directly to D2 without passing the server S.

The above provides an effective and user friendly mechanism for establishing Virtual Private Networks over generic IP connections. Broadcast services and service discovery protocols that normally require a direct layer-2 interconnection may work independently of the actual network structure. It also provides the possibilities of distributed network broadcast handling, where rules and configuration options may be cached in the end nodes of the network instead of in a centralised server. The described mechanism is unique in that it presents a complete distributed emulated LAN on top of an IP network where access and attributes such as security associations are completely controlled by a server. Most current solutions uses static tunnels. Either permanent connections are set up between the members of the VPN or tunnel servers which basically works as modem pools only you "dial" an IP number. This means that all traffic no matter it's final destination goes through this one box. In particular traffic going to sites in the VLAN (Virtual LAN) other than that of the VLAN server comes in through the server access and turns. The broadcast service allows service discovery protocols designed for local networks to function on the VPN while the ARP mechanism allows for dynamic establishment of secure tunnels directly between endpoints. The well known LANE (LAN Emulation) standard was focused entirely on ATM (Asynchronous Transfer Mode) and featured no integrated security handling. Lane introduces, inter alia, the ability to connect Ethernet and Token Ring networks together via ATM. LANE makes the process transparent, requiring no modification to Ethernet and Token Ring stations. LANE allows common protocols, such as IP, IPX, AppleTalk and DECnet, to ride over an ATM backbone. LAN emulation has been implemented and verified over ATM. However, since the system architecture itself by design avoids sending all data through the server, the bottleneck problem with overloaded server links is completely avoided.

In general, the present invention describes a decision scheme for a third-party overtaking of a client role in a two-party communication session. Turning to Fig. 1,

the system processes in the illustrated embodiment of the present invention comprises end user clients located at the end user premises equipment 1, a central VPN system server 2, and network edge located VPN system clients 3. Full lines indicate physical communication lines, whereas arrows indicate communicating ends, without specifying which route the communication takes between those communicating ends.

The end user client process 1 preferably resides in a PC, the VPN client 3 process preferably resides within a standalone hardware unit, and the VPN server process 2 preferably resides within any kind of server hardware unit, such as an IBM® server. By process is here meant the functionality for the particular client or server, as described herein. The VPN server 2 and the VPN client 3 are parts of a VPN system that provides the end user client 1 with access to required VPNs. The end user client 1 hardware is physically connected via a communication line 11 to the VPN client 3 hardware. The VPN client 3 hardware is physically connected to a layer-2 termination that enables the VPN client 3 to access Internet over a communication line 12. The layer-2 protocol is preferably Ethernet but could practically be any known layer-2 protocol used for the encapsulation and transport of IP (Internet Protocol) packets between IP nodes. The VPN server 2 is connected to the Internet via a communication line 13 in the same way as the VPN client 3.

According to an embodiment of the invention the end user client 1 initiates a communication session with the VPN server 2 in order to acquire access to a virtual private network. During the initialisation phase, the VPN server 2 authenticates and authorises the end user client 1 as a registered user of VPN services that are provided by the VPN server 2. The VPN client 3 is passive in that it does not initiate any new information elements during the initialisation phase. The VPN client 3 also monitors the communication 21 between the end user client 1 and the VPN server 2.

When the initialisation phase between the end user client 1 and the VPN server 2 is finished, and when information has been exchanged, regarding the particular VPN that the end user client requests access to, then the VPN client 3 becomes active and takes over the communication session between the end user client 1 and the VPN client 3. The VPN client 3 now requests, if it is necessary because the VPN information can already be cached by the VPN client 3, VPN configuration data from the VPN server 2. The VPN client 3 uses the configuration data to configure necessary VPN access parameters such as traffic classification parameters, performance assurance parameters, or firewall parameters such as encryption, authentication, filtering parameters, etc.

The end user client 1 is allowed to use different VPN servers 2 but cannot have simultaneous access to more than one VPN server 2. The VPN client 3 detects when

an end user client 1 tries to access a certain server 2. At this moment the VPN server 2 is considered insecure until the end user client 1 has authenticated the VPN server 2 and also have been authenticated by the VPN server 2.

The monitoring and session overtaking scenarios are described more in detail in Fig. 2. The VPN client 3 has one trusted domain, which is the end user client 1 side, and one distrusted domain, the Internet domain. From the VPN client's 3 point of view, the VPN server 2 is therefore located in the distrusted domain. Since all in- and outgoing IP traffic to/from the end user client passes through the VPN client 3 hardware, the VPN client 3 is able to monitor the communication 21 between the end user client 1 and the VPN server 2. This is true if, and only if, the IP traffic is not encrypted in such a way that the VPN client 3 is unable to decrypt the IP traffic. The VPN client 3 software resides on hardware that physically interconnects the end user client 1 with the Internet 4. The VPN client 3 is therefore able to monitor 22 all traffic 21 between the end user client 1 and different VPN servers 2 to whom the end user client 1 are registered as user.

The VPN client 3 identifies when the end user client 1 starts to establish contact with a VPN server 2. The VPN client 3 treats the end user client 1 side as a trusted party and the VPN server 2 as a distrusted party. The session establishment phase 21 between the end user client 1 and the VPN server 2 could be done in numerous ways, e.g. by a traditional challenge/response handshaking sequence. The communication 21 is primarily meant to be done by web based clients but other client/server process environment solutions are possible. When the handshaking sequence between the end user client 1 and the VPN server 2 has finished, the VPN client 3 takes over the communication session. The handshaking is considered finished when the VPN server 2 has authenticated and authorised the end user client 1, and acknowledged the end user client 1 as a confirmed user. The VPN client 3 will from now on undertake proxy roles towards both the end user client 1 and the VPN server 2. Towards the end user client 1, the VPN client 3 will act as a VPN server proxy, and towards the VPN server 2 as an end user client proxy. The end user client 1 will continue it's session in belief that it still communicates with the VPN server 2. The VPN client 3 will, using the VPN server proxy role, continue the VPN setup session with the end user client 1.

Further on, the VPN client 3 is now considering the VPN server 2 as a secure source and starts up communication sessions 23 with the VPN server 2 that enables the end user client 1 to be included as members in the requested VPN.

In one embodiment the invention is implemented in a service provisioning system, where parts of the service functionality are distributed to system clients acting as server proxies. One technical advantages of the present invention is that any hacker intrusions via an end user PC 1 are avoided by having critical

software/firmware for control and management of VPN configuration data separated on standalone hardware 3. Another advantage is the automated overtaking of certified sessions. Another benefit is the plug-and-play behavior for virtual services over Internet, which is made available through the invention. The teachings of the

5 present invention thus differs from prior art technology, since earlier solutions to the problem have either been centralised server solutions, such as PSTN/ISDN modem-pool solutions, server centralised IP Sec tunnelling etc, or distributed solutions, which are only valid within one network operator intra-domain or within federated network operator domains. These solutions are generally referred to as network

10 based VPN systems. The present invention will function independently of whether or not the different VPN client users access the same network operator domain or a federated network domain or have access to totally independent network operator domains.

Claims

1. System for establishment of a virtual private network connection, comprising an end user client (1) device and a VPN access server (2) communicatively connected
5 to the end user client via the Internet (4), **characterised in a standalone VPN client** (3) device physically interconnecting (11,12,13) the end user client with the Internet, said VPN client comprising monitoring means for monitoring (22) all traffic (21) between the end user client and the VPN server.
- 10 2. The system as recited in claim 1, wherein said monitoring means are devised to detect when a handshake agreement is established between the end user client and the VPN server.
3. The system as recited in claim 2, wherein said VPN client comprises session
15 overtaking means, devised to overtake a VPN setup session for said end user client upon detection of said handshake agreement.
4. The system as recited in claim 3, wherein the end unit client side of the VPN
20 client is defined as a secure domain, and the Internet and server side of the VPN client is defined as an insecure domain, said VPN client being devised only to accept a request for a VPN session setup when initialised from said secure domain.
5. The system as recited in claim 2, wherein said monitoring means are devised to
25 determine said handshake agreement for the VPN setup session as completed upon detecting that said server acknowledges a VPN setup request that has been initialised by said end user client.
6. The system as recited in claim 5, wherein said VPN client is devised to request,
30 upon detection of a completed handshake, said server to distribute VPN configuring data relevant for the inclusion of said end user client into said virtual private network.
7. The system as recited in claim 1, wherein said VPN client is devised to
35 undertake a proxy roll, comprising means for acting as a VPN server proxy towards the end user client, and means for acting as an end user client proxy towards the VPN server.
8. Method for establishing a connection for comprising an end user client (1) device to a virtual private network controlled by a VPN access server (2)

communicatively connected to the end user client via the Internet (4), comprising the steps of:

- providing a standalone VPN client (3) device physically interconnecting (11,12,13) the end user client with the Internet;
- 5 - monitoring (22) all traffic (21) between the end user client and the VPN server by means of monitoring means in said VPN client.

9. The method as recited in claim 8, wherein said monitoring means detects when a handshake agreement is established between the end user client and the VPN server.

10

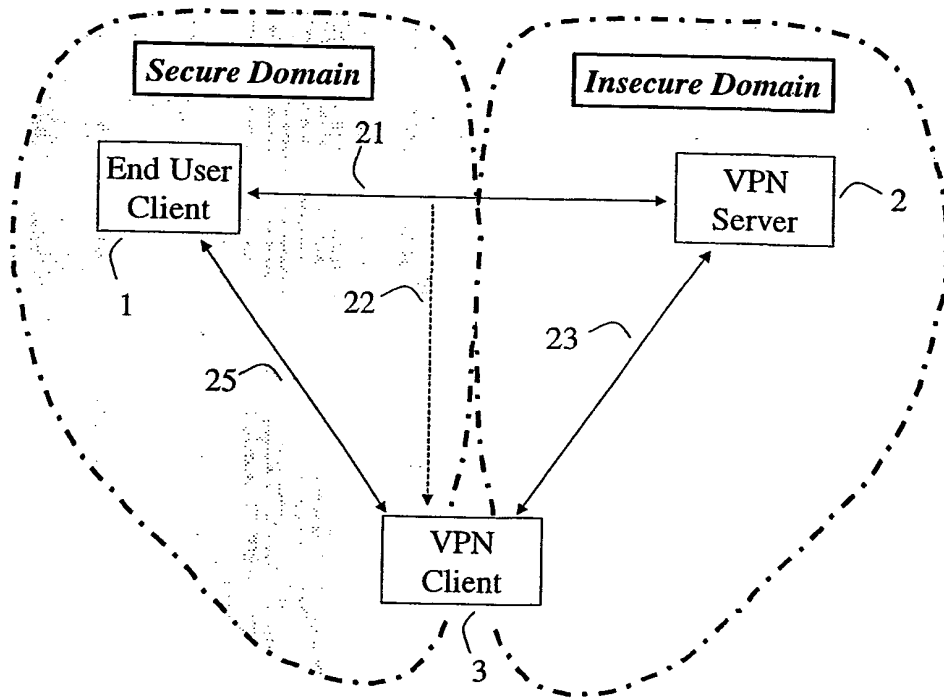
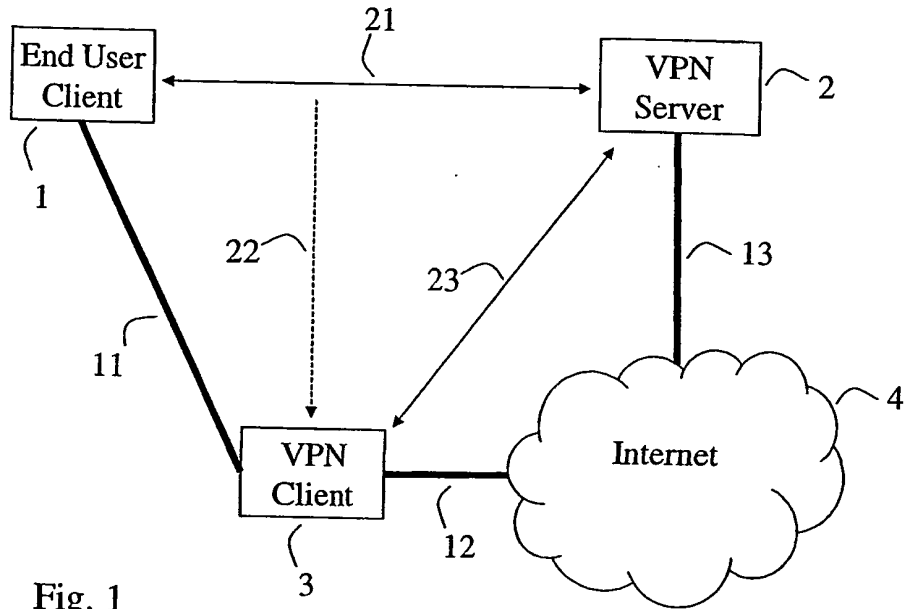
10. The method as recited in claim 9, wherein said VPN client overtakes a VPN setup session for said end user client upon detection of said handshake agreement.

11. The method as recited in claim 10, wherein the end unit client side of the VPN client is defined as a secure domain, and the Internet and server side of the VPN client is defined as an insecure domain, said VPN client only accepting a request for a VPN session setup when initialised from said secure domain.

12. The method as recited in claim 9, wherein said monitoring means determine said handshake agreement for the VPN setup session as completed upon detecting that said server acknowledges a VPN setup request that has been initialised by said end user client.

13. The method as recited in claim 12, wherein said VPN client requests, upon detection of a completed handshake, said server to distribute VPN configuring data relevant for the inclusion of said end user client into said virtual private network.

14. The method as recited in claim 1, wherein said VPN client undertakes a proxy roll, acting as a VPN server proxy towards the end user client, and acting as an end user client proxy towards the VPN server.



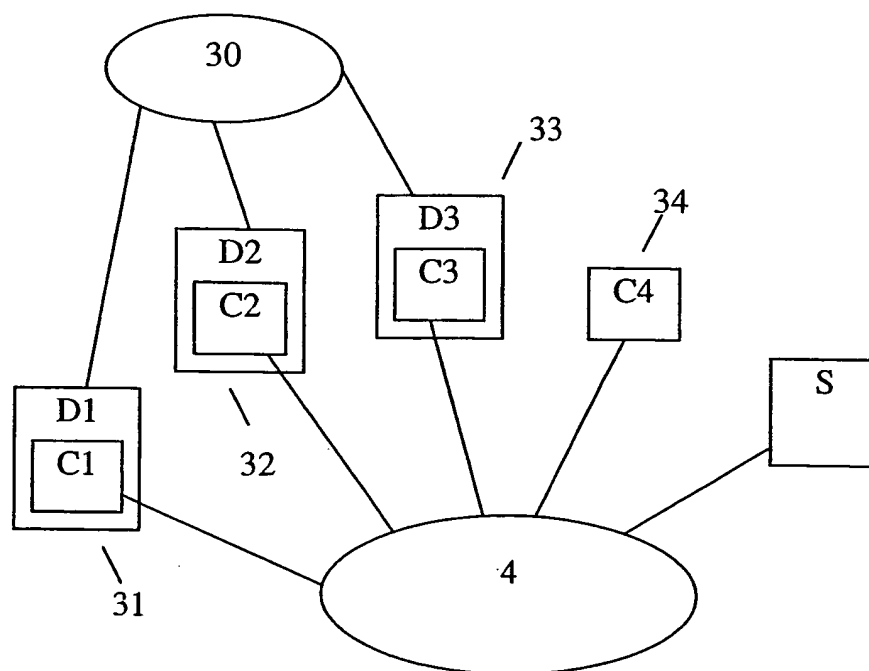


Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 01/01472

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 12/28, H04L 12/56, H04L 12/46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|-----------|---------------------------------------------------------------------------------------------------------|-----------------------|
| X | EP 1093255 A1 (ALCATEL), 18 April 2001 (18.04.01), whole document | 1-14 |
| | -- | |
| Y | WO 0651216 A1 (LODGENET ENTERTAINMENT CORP), 31 August 2000 (31.08.00), claims 1,14,24, abstract | 1-14 |
| | -- | |
| Y | US 6052788 A (WESINGER, JR. ET AL), 18 April 2000 (18.04.00), claim 1, abstract | 1-14 |
| | -- | |
| A | WO 9859467 A2 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)), 30 December 1998 (30.12.98), figure 2, abstract | 1-14 |
| | -- | |

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

4 February 2002

Date of mailing of the international search report

13-02-2002

Name and mailing address of the ISA/

Swedish Patent Office

Box 5055, S-102 42 STOCKHOLM

Facsimile No. +46 8 666 02 86

Authorized officer

Roger Bou Faisal/LR

Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/SE 01/01472

| Patent document cited in search report | | | Publication date | Patent family member(s) | | Publication date |
|-------------------------------------------|---------|----|---------------------|----------------------------|--------------|---------------------|
| EP | 1093255 | A1 | 18/04/01 | JP | 2001168918 A | 22/06/01 |
| WO | 0051216 | A1 | 31/08/00 | AU | 3609600 A | 14/09/00 |
| | | | | US | 6240533 B | 29/05/01 |
| US | 6052788 | A | 18/04/00 | US | 5898830 A | 27/04/99 |
| WO | 9859467 | A2 | 30/12/98 | AU | 7949998 A | 04/01/99 |
| | | | | SE | 513246 C | 07/08/00 |
| | | | | SE | 9702384 A | 24/12/98 |

This Page Blank (uspto)